

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

11-21-05

APR
IPW

PATENT APPLICATION

ATTORNEY DOCKET NO. 10005528 -1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): **Curtis Timothy Gross**

Confirmation No.: 6269

Application No.: 09/774844

Examiner: Nadia Khoshnoodi

Filing Date: Jan 31, 2001

Group Art Unit: 2133

Title: **Resource Sharing Across Security Boundaries**

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on Sept 19 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) \$500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month \$120 ☐ 2nd Month \$450 ☐ 3rd Month \$1020 ☐ 4th Month \$1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of \$ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, Alexandria, VA 22313-1450
Date of Deposit: 18 Nov 2005

OR

☐ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name: Carrie McKerley

Signature: *Carrie McKerley*

Respectfully submitted,

Curtis Timothy Gross

By *Philip S. Lyren*

Philip S. Lyren

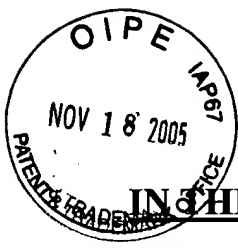
Attorney/Agent for Applicant(s)

Reg No. : 40,709

Date : 18 Nov 2005

Telephone : 281 514 8236

Express Mail Label No: EQ 350 018 988 US



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Curtis T. Gross	Examiner:	Nadia Khoshnoodi
Serial No.:	09/774,844	Group Art Unit:	2133
Filed:	January 31, 2001	Docket No.:	10005528-1
Title:	Resource Sharing Across Security Boundaries		

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is filed in response to the Final Office Action mailed June 20, 2005 and the Notice of Appeal filed on September 19, 2005.

AUTHORIZATION TO DEBIT ACCOUNT

It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's deposit account no. 08-2025.

11/22/2005 DTESSEM1 00000094 082025 09774844

01 FC:1402 500.00 DA

I. REAL PARTY IN INTEREST

The real party-in-interest is the assignee, Hewlett-Packard Company, a Delaware Corporation having its principal place of business in Palo Alto, California.

II. RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences known to appellant, the appellant's legal representative, or assignee that will directly affect or be directly affected by or have a bearing on the Appeal Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1 – 42 are finally rejected. No claims are allowed. The rejection of claims 1 – 42 is appealed.

IV. STATUS OF AMENDMENTS

In response to the OA dated 08/25/04, Applicant filed a response that included (among other claims) new claims 26-28. Each of these claims 26-28 included a typographical error. The Final OA dated 06/20/05 rejected claims 26-28 under 35 USC § 112, second paragraph. Applicant filed an amendment under 37 CFR 1.116 to correct the typographical errors in claims 26-28. Specifically, the word "descriptor" was changed to "description." No other amendments were presented.

A listing of pending claims appears in section VIII Claims Appendix. Claims 26-28 are presented with the typographical errors corrected (i.e., the word "descriptor" is changed to "description").

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations

from the specification and drawings should be read into the corresponding claim element or that these are the sole sources in the specification supporting the claim features.

Claim 1

A method for sharing resources between first and second workstations separated by a segment of a public network, the method comprising (FIGS. 2-5):

transmitting an email message (FIG. 2: #102) from said first workstation (FIG. 2: #101) to said second workstation (FIG. 4: #401) separated from said first workstation by at least one security measure (FIG. 2: #104) disposed within a destination computing site (FIG. 2: #201; p. 7, lines 1-20);

employing a protocol to enable said transmitted email message to penetrate said at least one security measure (p. 7, lines 7-20; p. 9, line 1 - p. 10, line 5);

determining, by said second workstation, if an executable command is within a script of the email message (p. 7, lines 21-27; p. 11, lines 11-23); and

executing the command if within said script of the email message (p. 7, lines 21-27; p. 8, lines 9-29; p. 12, lines 9-18).

Claim 15

A system for securely enabling resource sharing among a plurality of workstations over a public network, the system comprising (FIGS. 2-5):

means for transmitting an email message (FIG. 2: #102) from a first workstation (FIG. 2: #101) of said plurality of workstations onto said public network (FIG. 3: #301; p. 7, lines 1-20);

means for enabling said transmitted email message to pass through a firewall (FIG. 2: #104) separating said public network from a second workstation (p. 7, lines 7-20; p. 9, line 1 - p. 10, line 5);

means for receiving said transmitted email message at a second workstation (FIG. 4: #401; FIG. 5: #503; p. 11, lines 11-23);

means for verifying an authorization of said first workstation to request execution, at said second workstation, of a selected function included in a script in the email message (p. 11, line 11 - p. 12, line 29); and

means for automatically performing said selected function at said second workstation if said authorization of said first workstation is verified (p. 11, line 11 – p. 12, line 29).

Claim 16

The system of claim 15 wherein performing said selected function includes executing code already resident on said second workstation (p. 11, line 24 – p. 12, line 18).

Claim 23

A system for causing a function to be performed at a destination computing site remote from a requesting computing site, the system comprising (FIGS. 2-5):

an email composer disposed in communication with said requesting computing site for composing an email message including a task description and authenticating data, wherein the authenticating data authenticates said requesting computing site (p. 9, line 1 – p. 10, line 5;

a network link (FIG. 3: #310) for enabling transmission of said composed email message (p. 10, lines 6-25);

a mail gateway (FIG. 2: #105) disposed in communication with said destination computing site for receiving said transmitted composed email (p. 10, lines 6-25);

a mail server (FIG. 2: #201) dedicated to a destination computing device disposed within said destination computing site for identifying said task description (p. 7, lines 7-27; p. 10, line 26 – p. 11, line 10);

means for verifying said authenticating data (p. 9, line 1 – p. 10, line 5; p. 11, line 1 – p. 12, line 2); and

means for executing said described task where said authenticating data is verified (p. 12, lines 9-18).

Claim 29

A method, comprising (FIGS. 2-5);
transmitting an email (FIG. 2: #102) from a first workstation (FIG. 2: #101),
through a firewall (FIG. 2: #104), to a second workstation (FIG. 4: #401; p. 7, lines 1-20);
automatically detecting, by the second workstation, if an executable file is
attached to the email (p. 7, lines 21-27; p. 11, lines 11-23); and
automatically executing, at the second workstation, the executable file attached to
the email (p. 7, lines 21-27; p. 8, lines 9-29; p. 12, lines 9-18).

Claim 33

The method of claim 29 wherein automatically executing the executable file
causes the second workstation to execute code already resident on the second workstation
(p. 11, lines 11-23; p. 12, lines 9-18).

Claim 37

A method, comprising (FIGS. 2-5):
transmitting an email (FIG. 2: #102) from a first workstation (FIG. 2: #101) to a
second workstation (FIG. 4: #401; p. 7, lines 1-20);
automatically examining, at the second workstation, the email to determine if an
executable instruction is (i) within a body of the email or (ii) within an attachment to the
email (p. 7, lines 21-27; p. 11, lines 11-23); and
if the executable instruction is present, then automatically executing, at the second
workstation, the executable instruction (p. 7, lines 21-27; p. 8, lines 9-29; p. 12, lines 9-18).

Claim 38

The method of claim 37 wherein the executable instruction is a script included
within the body of the email (p. 8, lines 9-16).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 26-28 are rejected under 35 USC § 112, second paragraph, as being indefinite for lacking antecedent basis.

II. Claims 1-2, 4-9, and 13-25 are rejected under 35 U.S.C. §103(a) as being unpatentable over USPN 5,680,461 (McManis) in view of USPN 5,710,883 (Hong).

III. Claims 3, 12, 16, and 28 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Hong in view of JP Pub. No. 2000-162926 (Tetsuro).

IV. Claims 10-11 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Hong in view of USPN 5,960,177 (Tanno).

V. Claims 29-30, 32-35, and 37-42 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis in view of Tetsuro.

VI. Claims 31 and 40 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Tetsuro in view of USPN 6,389,121 (Terao).

VII. Claim 36 is rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Tetsuro in view of Tanno.

VII. ARGUMENT

The rejection of claims 1 – 42 is improper, and Applicant respectfully requests reversal of this rejection.

The claims do not stand or fall together. Instead, Applicant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

I. Claims 26-28

Claims 26-28 are rejected under 35 USC § 112, second paragraph, as being indefinite for lacking antecedent basis. In response to this rejection, Applicant filed an amendment after final under 37 CFR 1.116 to correct typographical errors in claims 26-28.

II. Claims 1-2, 4-9, and 13-25

Claims 1-2, 4-9, and 13-25 are rejected under 35 U.S.C. § 103(a) as being unpatentable over USPN 5,680,461 (McManis) in view of USPN 5,710,883 (Hong). Applicant respectfully traverses and argues claim 1.

Overview of McManis

McManis teaches systems and methods for sending data packets between two entities in a network (2: 1-10). In network communications, messages are sent as data packets that contain a header, a payload, and a trailer (4: 16-20). McManis teaches that his packets contain executable code in the language of virtual machine modules of the client, firewall, and server (4: 52-55). Some of this executable code can be “executed by the server computer to perform a particular function” (4: 57-62). Thus, McManis teaches that the data **packets themselves contain executable code**.

Overview of Hong

Hong teaches a method for publishing a hypertext file set on a world-wide web server (3: 34-35). First, the hypertext file is packaged as an email message, and the email is transported over the internet from a client machine to the world-wide web server (3: 36-39). The world-wide web server unpacks the email, recovers the original hypertext file, and stores the file (3: 39-43).

A. Claim 1

The combination of McManis and Hong does not teach or suggest all the elements of claim 1. Claim 1 recites that an email is transmitted from a first work station to a second workstation. Then, the second workstation determines “if an executable command is **within a script of the email message**” (emphasis added). If the executable command is within the script of the email message, then the command is executed. McManis in view of Hong does not teach or suggest these recitations.

As noted above, data packets contain a header, a payload, and a trailer. McManis expressly teaches that the data packets themselves contain executable code. Hong teaches that hypertext files are packaged as an email and sent over the internet. By contrast, claim 1 recites transmitting an email from a first workstation to a second workstation. The second workstation determines if an executable command is “within a script of the email message.” Transmitting data packets containing executable code is completely different than determining, by a workstation, if an executable command is within a script of an email message.

The Examiner argues that McManis and Hong teach or suggest claim 1. For several reasons, Applicant disagrees. First, nowhere does McManis or Hong teach or suggest that executable commands are actually placed “within a script of an email.”

Second, Applicant respectfully request that words in a claim be given their plain meaning (i.e., the ordinary and customary meaning given to the term by one of ordinary skill in the art: see MPEP § 2111.01). Specifically, the words “script” and “packet” have two entirely different meanings to one of ordinary skill in the art. Webopedia is an online dictionary (www.webopedia.com) dedicated to providing computer and internet technology definitions. Webopedia defines “script” and “packet” as follows:

Script: Another term for macro or batch file, a script is a list of commands that can be executed without user interaction. A *script language* is a simple programming language with which you can write scripts.

Packet: A piece of a message transmitted over a packet-switching network. See under packet switching. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called *datagrams*.

Applicant further respectfully asks the Board of Appeals to interpret the term "script" in light of the specification. A portion of Applicant's specification discussing scripts is reproduced below:

In a preferred embodiment, scripts may be included in the email message having an included task or function in order to appropriately instruct a destination workstation what operations to perform in response to an incoming email message. The contents of such scripts will generally vary depending on several factors including but not limited to: the type of task included in the email message, the nature of the device and/or program intended to execute the task, and the nature, if any, of any encryption employed in encoding the email message. The desired scripts may be generated employing common scripting languages or employing a scripting language developed for a particular application.

In a preferred embodiment, scripts recognizable to commonly used software routines may be employed in order to enable specific tasks to be precisely identified with a minimum of identifying terms. One example of this practice is the use of "primary verbs" within Microsoft Networks.RTM.. Employing this program, any

file name ending with a ".doc" extension is preferably recognized as a document for which a common operation is printing. For example, where it is desired to print a document, employing the scripting term "print" would cause the receiving workstation to open a document, print it, and then close the document, all in response to the single term "print." In this manner, the inventive system may economize on the number of commands to be communicated to the destination device without omitting any specificity in describing the actions to be taken upon receipt on an email message. It will be appreciated that the document to be printed could either be transmitted as an attachment to a transmitted email and/or be resident within a network accessible to a workstation receiving the "print" command. (p. 8, lines 9-29)

In light of Applicant's specification and dictionary definitions, McManis and Hong do not teach or suggest the elements of claim 1. McManis teaches that packets can contain executable code. Hong teaches that hypertext files are packaged as emails and sent over the internet. By contrast, claim 1 recites that a workstation receives an email and then determines if an executable command is "within a script of the email message."

Applicants further argue that the Examiner is improperly using the terms "script" and "packet" as being synonyms or analogous. While arguing that McManis teaches the limitations of claim 1, the Examiner states: "Inherently in this process, there must be a determination that an executable command exists in the payload, i.e., script, of the packet in order to execute it" (see FOA at p. 5). Here, the Examiner improperly equates a script with a packet.

For at least these reasons, the independent claims are allowable over the art of record. The dependent claims are allowable for at least these reasons.

B. Claim 16

Claim 15 (from which claim 16 depends) recites that an email is transmitted from a first workstation to a second workstation. The second workstation verifies authorization

to execute a selected function in a script of the email. According to claim 16, performing this selected function “includes executing code already resident on said second workstation.” McManis and Hong do not teach or suggest these recitations.

McManis expressly teaches that data packets are embedded with source, destination, and main methods that contain executable code (4: 48-55). The packets are sent to their destination and executed (4: 57-62). McManis never states or even suggests that additional executable code is already resident at the destination. The Examiner cites FIG. 6, element 632 of McManis (see FOA at p. 9). This figure actually supports the position of the Applicant. As shown in FIG. 6, the server receives (at box 626) the packet object. If the packet object is acceptable (box 628), then the server executes the main method to implement the desired function (box 632). McManis, however, expressly teaches that the main method is embedded in the packets, not resident at the server computer (see 4: 48-62).

III. Claims 3, 12, 16, and 28

Claims 3, 12, 16, and 28 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Hong in view of JP Pub. No. 2000-162926 (Tetsuro). Applicant respectfully traverses.

No Suggestion/Motivation to Modify/Combine References

No suggestion or motivation exists to modify or combine McManis and Hong with Tetsuro because Tetsuro actually teaches away from McManis. McManis teaches that the server receives the data packet having executable code. The server, and not a user, determines if the packet is acceptable (7: 5-23). If the server determines that the packet is acceptable, then the server (and not a user) executes the main method portion of the packet (7: 24-36). By contrast, Tetsuro expressly teaches that a user determines whether to execute a file attached to an email. For example, the Abstract of Tetsuro states: “To execute a proper diagnosis or control function, the **users can execute** a file attached to a received e-mail message” (emphasis added). As another example, FIGS. 12 and 15 in Tetsuro show an email message being displayed to a user. The email message

instructs the user how to proceed: "Please double-click on the attached executable file which will allow us to test analyze your printer."¹

In contrast to Tetsuro, claim 1 recites that the second workstation determines if an executable command is within a script in the email message. In other words, a machine (i.e., the second workstation) determines whether to execute a script in an email. By contrast, Tetsuro expressly teaches that a user determines whether to execute a file attached to an email.

The Examiner must provide *objective evidence*, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Such teaching or suggestion does not exist.

For at least these reasons, Applicant respectfully asks the Board of Appeals to withdraw the rejection since a *prima facie* case of obvious has not been established.

IV. Claims 10-11

Claims 10-11 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Hong in view of USPN 5,960,177 (Tanno).

Dependent claims 10-11 depend from independent claim 1 and, thus, inherit all the limitations of the independent base claim. As noted above, McManis and Hong do not teach or suggest all the recitations in claim 1. Tanno fails to cure the deficiencies of McManis and Hong. For at least these reasons, claims 10 and 11 are allowable over McManis and Hong in view of Tanno.

V. Claims 29-30, 32-35, and 37-42

Claims 29-30, 32-35, and 37-42 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis in view of Tetsuro. Applicant respectfully traverses.

¹ Applicant relies on an English translation of Tetsuro which was filed in Japanese.

No Suggestion/Motivation to Modify/Combine References

No suggestion or motivation exists to modify or combine McManis and Tetsuro because Tetsuro actually teaches away from McManis. McManis teaches that the server receives the data packet having executable code. The server, and not a user, determines if the packet is acceptable (7: 5-23). If the server determines that the packet is acceptable, then the server (and not a user) executes the main method portion of the packet (7: 24-36). By contrast, Tetsuro expressly teaches that a user determines whether to execute a file attached to an email. For example, the Abstract of Tetsuro states: "To execute a proper diagnosis or control function, the **users can execute** a file attached to a received e-mail message" (emphasis added). As another example, FIGS. 12 and 15 in Tetsuro show an email message being displayed to a user. The email message instructs the user how to proceed: "Please double-click on the attached executable file which will allow us to test analyze your printer."

The Examiner must provide *objective evidence*, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Such teaching or suggestion does not exist.

For at least these reasons, Applicant respectfully asks the Board of Appeals to withdraw the rejection since a *prima facie* case of obvious has not been established.

All Elements Not Taught or Suggested

The combination of McManis and Tetsuro does not teach or suggest all the elements of the claims.

A. Claims 29 and 37

Claim 29 recites that the second workstation **automatically** detects if an executable file is attached to the email and **automatically** executes the file. In other words, a machine (i.e., the second workstation) automatically detects and executes an

executable file. Claim 37 recites **automatically** examining at the second workstation and **automatically** executing at the second workstation. By contrast, Tetsuro expressly teaches that a user determines whether to execute a file attached to an email. Nowhere does Tetsuro teach or suggest that a machine (i.e., a computer or workstation) automatically examines and then executes an executable file or instructions as claimed.

Second, Applicant respectfully request that words in a claim be given their plain meaning (i.e., the ordinary and customary meaning given to the term by one of ordinary skill in the art: see MPEP § 2111.01). Merriam-Webster is an online dictionary (www.merriam-webster.com) that defines “automatic” as follows:

automatic: largely or wholly involuntary; *especially* : **REFLEX** 5
<automatic blinking of the eyelids> **b** : acting or done
spontaneously or unconsciously **c** : done or produced as if by
machine.

Applicant further respectfully asks the Board of Appeals to interpret the term “automatic” in light of the specification. Exemplary portions of Applicant’s specification discussing “automatic” are reproduced below:

In this manner, the inventive server software may be employed to automatically execute tasks which previously would have required user intervention. (P. 4, lines 14-16).

In addition, the server software disposed either within or in communication with workstation 503 preferably includes the ability to run executable files attached to email messages (or take appropriate actions on other file types such as documents) arriving at workstation 503 without a need for human intervention, i.e. automatically. (P. 11, lines 14-18).

In light of Applicant's specification and dictionary definitions, McManis and Tetsuro do not teach or suggest the elements of claim 29 and 37.

For at least these reasons, the independent claims are allowable over the art of record. The dependent claims are allowable for at least these reasons.

B. Claim 33

Claim 33 recites that automatically executing the file causes the second workstation to execute code already resident on the second workstation. McManis and Tetsuro do not teach or suggest this recitation.

McManis expressly teaches that data packets are embedded with source, destination, and main methods that contain executable code (4: 48-55). The packets are sent to their destination and executed (4: 57-62). McManis never states or even suggests that additional executable code is already resident at the destination. As shown in FIG. 6, the server receives (at box 626) the packet object. If the packet object is acceptable (box 628), then the server executes the main method to implement the desired function (box 632). McManis, however, expressly teaches that the main method is embedded in the packets, not resident at the server computer (see 4: 48-62).

Nowhere does Tetsuro teach or suggest that code is already resident on the second workstation that executes the file.

C. Claim 38

Claim 38 recites that the executable code is a script included within a body of the email. The Examiner argues that Tetsuro teaches this recitation. Applicant respectfully disagrees.

Tetsuro teaches that a user is sent an email with a text message. For example, FIGS. 12 and 15 in Tetsuro show an email message being displayed to a user. The email message instructs the user how to proceed: "Please double-click on the attached executable file which will allow us to test analyze your printer." Asking a user to double-click on a file does not teach or suggest providing a script in the body of an email.

Applicant respectfully request that words in a claim be given their plain meaning (i.e., the ordinary and customary meaning given to the term by one of ordinary skill in the art: see MPEP § 2111.01). Specifically, Webopedia defines “script” as follows:

Script: Another term for macro or batch file, a script is a list of commands that can be executed without user interaction. A *script language* is a simple programming language with which you can write scripts.

Applicant further respectfully asks the Board of Appeals to interpret the term “script” in light of the specification (see Applicant’s specification at p. 8, lines 9-29, reproduced above).

In light of Applicant’s specification and dictionary definitions, McManis and Tetsuro do not teach or suggest that the executable code is a script included within a body of the email.

VI. Claims 31 and 40

Claims 31 and 40 are rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Tetsuro in view of USPN 6,389,121 (Terao).

Dependent claims 31 and 40 depend from independent claims 29 and 37 and, thus, inherit all the limitations of the respective independent base claim. As noted above, McManis and Tetsuro do not teach or suggest all the recitations in claims 29 and 37. Terao fails to cure the deficiencies of McManis and Tetsuro. For at least these reasons, claims 31 and 40 are allowable over McManis and Tetsuro in view of Terao.

VII. Claim 36

Claim 36 is rejected under 35 U.S.C. §103(a) as being unpatentable over McManis and Tetsuro in view of Tanno. For at least the reasons given in connection with independent claim 29, dependent claim 36 is allowable over the art of record.

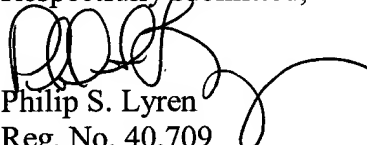
CONCLUSION

In view of the above, Applicant respectfully requests the Board of Appeals to reverse the Examiner's rejection of all pending claims.

Any inquiry regarding this Amendment and Response should be directed to Philip S. Lyren at Telephone No. (281) 514-8236, Facsimile No. (281) 514-8332. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,


Philip S. Lyren
Reg. No. 40,709
Ph: 281-514-8236

CERTIFICATE UNDER 37 C.F.R. 1.10

The undersigned hereby certifies that this paper or papers, as described herein, is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to: Commissioner for Patents, Alexandria VA 22313-1450 on this 18th day of November, 2005.

By 
Name: Carrie McKerley

Express Mail Label No. EQ 350 018 988 US

VIII. Claims Appendix

1. A method for sharing resources between first and second workstations separated by a segment of a public network, the method comprising:

transmitting an email message from said first workstation to said second workstation separated from said first workstation by at least one security measure disposed within a destination computing site;

employing a protocol to enable said transmitted email message to penetrate said at least one security measure;

determining, by said second workstation, if an executable command is within a script of the email message; and

executing the command if within said script of the email message.

2. The method of claim 1 wherein said protocol is SMTP (Simple Mail Transfer Protocol).

3. The method of claim 1 wherein said step of executing said command causes the second workstation to perform one of printing a document attached to the email message, generating a calendar entry on the second workstation, and running a diagnostic program on said second workstation.

4. The method of claim 1 wherein said executing step comprises the step of: performing an operation on data other than said transmitted email message.

5. The method of claim 1 further comprising the step of: at said second workstation, verifying an identity of said first workstation.

6. The method of claim 1 wherein said at least one security measure is a firewall.

7. The method of claim 6 further comprising the step of:

disposing said destination computing site within a controlled-access network.

8. The method of claim 7 further comprising the step of:
disposing said firewall in between said public network and said controlled-access network.

9. The method of claim 7 further comprising the step of:
attaching an executable file to said message, wherein said executing step comprises the step of:
executing said attached executable file.

10. The method of claim 1 wherein said executing step comprises the step of:
executing a routine resident in a controlled-access network identified in said email message.

11. The method of claim 10 wherein said step of executing comprises the step of:
running a diagnostic program at said second workstation.

12. The method of claim 1 wherein said executing step causes said second workstation to print a document attached to the email message.

13. The method of claim 1 wherein said executing step comprises the step of:
performing an operation on a document attached to said transmitted email message.

14. The method of claim 1 wherein said executing step comprises the step of:
performing an operation on a document resident within said destination computing site.

15. A system for securely enabling resource sharing among a plurality of workstations over a public network, the system comprising:

means for transmitting an email message from a first workstation of said plurality of workstations onto said public network;

means for enabling said transmitted email message to pass through a firewall separating said public network from a second workstation;

means for receiving said transmitted email message at a second workstation;

means for verifying an authorization of said first workstation to request execution, at said second workstation, of a selected function included in a script in the email message; and

means for automatically performing said selected function at said second workstation if said authorization of said first workstation is verified.

16. The system of claim 15 wherein performing said selected function includes executing code already resident on said second workstation.

17. The system of claim 15 wherein said means for enabling comprises:
an SMTP (Simple Mail Transfer Protocol) port for enabling communication of said message through said firewall.

18. The system of claim 15 further comprising:
a mail server dedicated to said second workstation; and
means for enabling communication between said dedicated mail server and said second workstation.

19. The system of claim 15 wherein said means for verifying said authorization comprises:

means for generating a digital signature at said first workstation; and

means for decrypting said digital signature at said second workstation.

20. The system of claim 15 wherein said means for automatically performing comprises:

means for running an executable file attached to said message.

21. The system of claim 15 wherein said means for automatically performing comprises:

means for running an executable file identified in said message and resident in a controlled-access network.

22. The system of claim 15 wherein said means for automatically performing comprises:

means for performing an operation on a document attached to said message.

23. A system for causing a function to be performed at a destination computing site remote from a requesting computing site, the system comprising:

an email composer disposed in communication with said requesting computing site for composing an email message including a task description and authenticating data, wherein the authenticating data authenticates said requesting computing site;

a network link for enabling transmission of said composed email message;

a mail gateway disposed in communication with said destination computing site for receiving said transmitted composed email;

a mail server dedicated to a destination computing device disposed within said destination computing site for identifying said task description;

means for verifying said authenticating data; and

means for executing said described task where said authenticating data is verified.

24. The system of claim 23 wherein said authenticating data includes a digital signature.

25. The system of claim 23 wherein said destination computing site is coupled to a local area network.

26. The system of claim 23 wherein said task description is a script having instructions to the means for executing.

27. The system of claim 23 wherein said task description is included in text of the email message.

28. The system of claim 23 wherein said task description is an instruction to print a document attached to the email message.

29. A method, comprising;
transmitting an email from a first workstation, through a firewall, to a second workstation;
automatically detecting, by the second workstation, if an executable file is attached to the email; and
automatically executing, at the second workstation, the executable file attached to the email.

30. The method of claim 29 wherein automatically executing the executable file causes the second workstation to print a document attached to the email.

31. The method of claim 29 wherein automatically executing the executable file causes the second workstation to print a document located within a network that is accessible to the second workstation.

32. The method of claim 29 wherein automatically executing the executable file causes the second workstation to print the email.

33. The method of claim 29 wherein automatically executing the executable file causes the second workstation to execute code already resident on the second workstation.

34. The method of claim 29 wherein automatically executing the executable file causes the second workstation to execute code at a device in communication with the second workstation.

35. The method of claim 29 wherein automatically executing the executable file causes the second workstation to execute code included as an attachment to the email.

36. The method of claim 29 wherein automatically executing the executable file causes the second workstation to execute a file resident within a network, the file being accessible to the second workstation but not within the second workstation.

37. A method, comprising:
transmitting an email from a first workstation to a second workstation;
automatically examining, at the second workstation, the email to determine if an executable instruction is (i) within a body of the email or (ii) within an attachment to the email; and
if the executable instruction is present, then automatically executing, at the second workstation, the executable instruction.

38. The method of claim 37 wherein the executable instruction is a script included within the body of the email.

39. The method of claim 37 wherein the executable instruction instructs the second workstation to print a document to a specific printer.

40. The method of claim 37 wherein the executable instruction instructs the second workstation to print a document in a specific format.

41. The method of claim 37 wherein the executable instruction instructs the second workstation to execute a routine located within a network to which the second workstation is connected.

42. The method of claim 37 wherein the executable instruction instructs the second workstation to print a document attached to the email.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.